UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,293	12/05/2003	Raymond Harper	030250; 190250-1500	2178

38823 7590 01/25/2011
AT&T Legal Department - TKHR
Attn: Patent Docketing
One AT&T Way
Room 2A-207
Bedminster, NJ 07921

EXAMINER	
ALMEIDA, DEVIN E	
ART UNIT	**PAPER NUMBER**
2432	
MAIL DATE	**DELIVERY MODE**
01/25/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RAYMOND HARPER

Appeal 2009-007148
Application 10/729,293[1]
Technology Center 2400

Before JAY P. LUCAS, JOHN A. JEFFERY, and CAROLYN D. THOMAS, *Administrative Patent Judges*.

LUCAS, *Administrative Patent Judge*.

DECISION ON APPEAL[2]

[1] Application filed December 5, 2003. The real party in interest is AT&T.

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

Appellant appeals from a final rejection of claims 1 to 29 under authority of 35 U.S.C. § 134(a). The Board of Patent Appeals and Interferences (BPAI) has jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Appellant's invention relates to a password management system for a switched access remote test system (SARTS) that tests frame relay circuits (Spec. 2, ll. 4 to 5). The graphical overlay for the UNIX-based program permits users to change their passwords more efficiently (Spec. 12, ll. 13 to 15). In the words of Appellant:

> If the user wishes to change his or her password, the password manager sends a change password request to the server … . Again, the password manager typically awaits a response from the server … . The response from the server typically comes in numerous forms based upon the server or the time of day. … The password manager then checks the response against the expected results.

(Spec. 13, l. 22 to 14, l. 8).

The following claim illustrates the claims on appeal:

Claim 1:

> 1. A password management system, comprising:
>
> graphical user interface logic residing on a first computer system operable to receive a current password from a user, prompt the user to determine whether the user desires to change the

> current password, and responsive to the user response receive a new password;
>
> password configuration logic residing on the first computer system operable to confirm the current password associated with the user on a switched access remote test system residing on a second computer system remote from the first computer system;
>
> password administration logic residing on the first computer system, responsive to the password confirmation logic and the graphical user interface, operable to receive the new password and to change the current password on the switched access remote test system; and
>
> expiration logic residing on the first computer system operable to determine if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system and is operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Ackroff	US 5,105,438	Apr. 14, 1992
Kadooka	US 5,606,663	Feb. 25, 1997
Goldberg	US 5,748,890	May 05, 1998
Limsico	US 5,793,952	Aug. 11, 1998

REJECTIONS

The Examiner rejects the claims as follows:

R1: Claims 1 to 10 and 12 to 29 stand rejected under 35 U.S.C. § 103(a) for being obvious over Limsico in view of Ackroff further in view of Kadooka.

R2: Claim 11 stands rejected under 35 U.S.C. § 103(a) for being obvious over Limsico in view of Ackroff further in view of Kadooka further in view of Goldberg.

We have only considered those arguments that Appellant actually raised in the Brief. Arguments Appellant could have made but chose not to make in the Brief have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

ISSUE

The issue is whether Appellant has shown that the Examiner erred in rejecting the claims under 35 U.S.C. § 103(a). The issue specifically turns on whether Limsico and Kadooka render obvious Appellant's claim limitation "expiration logic residing … operable to determine if the current password is approaching its expiration … and … operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration." (Claim 1).

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence.

Disclosure

1. Appellant has invented a system, method, and medium for password management on a distributed computing network (Spec. 2, l. 5; Fig. 1). Appellant's claimed system includes expiration logic that determines if a current user password is approaching expiration (claim 1). The claimed "expiration logic" prompts a user to change the current password when the current password is near expiration (*id.*).

Limsico

2. The Limsico reference discloses a password management system on a distributed computing network. Limsico's system includes password aging that determines if a current user password is approaching expiration. Limsico's password aging prompts a user to change the current password when the current password is near expiration (col. 9, ll. 34 to 40).

Kadooka

3. The Kadooka reference discloses a password management system (col. 1, ll. 6 to 9). Kadooka further discloses determining if a current user password is approaching expiration and prompting a user to change the current password when the current password approaches expiration (col. 1, ll. 49 to 57).

PRINCIPLE OF LAW

Appellant has the burden on appeal to the Board to demonstrate Examiner error. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006).

ANALYSIS

Arguments with respect to the rejection of claims 1 to 10 and 12 to 29 under 35 U.S.C. § 103(a) [R1]

The Examiner has rejected the noted claims for being obvious over Limsico, Ackroff, and Kadooka, pages 3 to 10 of the Examiner's Answer.

Appellant argues that the Limsico and Kadooka references describe a host computer of a password protected computer system having password routines residing on the host computer of the password protected computer system (Brief 10, middle). These password routines of Limsico and Kadooka do not reside on a second computer, according to Appellant (*id.*). Thus, the proposed combination does not teach all of the limitations of claim 1 (*id.*).

We disagree with Appellant's argument for the following reasons. We find that Appellant has invented a system, method, and medium for password management on a distributed computing network (FF#1). Appellant's claimed system includes expiration logic that determines if a current user password is approaching expiration (*id.*). Appellant's claimed "expiration logic" prompts a user to change the current password when the current password is near expiration (*id.*). In comparison, we find that the Limsico reference discloses a password management system on a distributed computing network (FF#2). We find that Limsico's system includes password aging (*i.e.*, Appellant's claimed expiration logic) that determines if a current user password is approaching expiration (*id.*). We find that Limsico's password aging prompts a user to change the current password when the current password is near expiration (*id.*).

In addition, we find that the Kadooka reference discloses a password management system (FF#3). Kadooka further discloses determining if a current user password is approaching expiration and prompting a user to change the current password when the current password approaches expiration (*id.*).

In *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 402 (2007), the Supreme Court identified circumstances in which a combination of elements (*i.e.*, a sensor on an adjustable pedal in a car) would have been obvious to try. More specifically, the Court stated: "When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill in the art has good reason to pursue the known options within his or her technical grasp." *Id.* at 421.

We apply *KSR*'s teachings to the facts on the record before us. Here, there is a design need to ensure a user's ability to change passwords (*i.e.*, to provide enterprise-based solutions) in the SARTS system. The need is fulfilled by designing Appellant's claimed "expiration logic" on a distributed computing system. Yet, only a finite number of ways exist in which a person of ordinary skill in the art would have arranged Appellant's claimed "expiration logic." That is, the claimed "expiration logic" would have been configured by a skilled artisan either remotely or locally located relative to the switched access remote testing system (SARTS). Given the design need to provide enterprise-based solutions on different computers (*e.g.*, via a network), we find that there would have been a finite number of identified, predictable solutions (*e.g.*, placement of the expiration logic on the claimed "first computer system" or the claimed "second computer system") that would have been within the technical grasp of the skilled artisan. In accordance with the teachings of *KSR* as applied in the above-stated analysis, we find that Appellant's claimed "expiration logic residing … operable to determine if the current password is approaching its expiration … and … operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration" (claim 1) is rendered obvious by the combination of Limsico and Kadooka. We thus conclude Appellant has not shown error in the rejection of claim 1.

Regarding claims 12 to 29, Appellants make separate arguments in accordance with 37 C.F.R. § 41.37(c)(1)(vii). (*See* App. Br. 12 to 18). However, the arguments are the same as those already addressed above with respect to claim 1. Therefore, we will not repeat the arguments here. Claims 12 to 29 fall for the same reasons as described for claim 1.

Argument with respect to the rejection of claim 11 under 35 U.S.C. § 103(a) [R2]

The Examiner has rejected claim 11 for being obvious over Limsico, Ackroff, Kadooka, and Goldberg, pages 10 to 11 of the Examiner's Answer.

Appellant makes no separate arguments in accordance with 37 C.F.R. § 41.37(c)(1)(vii). Accordingly, we affirm the rejection R2.

CONCLUSION OF LAW

Based on the findings of facts and analysis above, we conclude that Appellant has not shown that the Examiner erred in rejecting claims 1 to 29.

DECISION

We affirm the Examiner's rejections R1 and R2 of claims 1 to 29.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

peb

AT&T LEGAL DEPARTMENT – TKHR
ATTN: PATENT DOCKETING
ONE AT&T WAY
ROOM 2A-207
BEDMINSTER, NJ 07921